#3

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed th this Office.

出 願 年 月 日
Date of Application: ２０００年　６月２９日

願 番 号
Application Number: 特願２０００－１９６０４０

願 人
Applicant (s): 富士通株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２０００年　９月２２日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願
【整理番号】　0051220
【提出日】　平成12年 6月29日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 9/00
G09C 1/00
【発明の名称】　暗号制御装置
【請求項の数】　5
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　関　裕二
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　川崎　雄介
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　橋本　繁
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　柳　良一
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100094330

【弁理士】

【氏名又は名称】　山田　正紀

【選任した代理人】

【識別番号】　100109689

【弁理士】

【氏名又は名称】　三上　結

【手数料の表示】

【予納台帳番号】　017961

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9912909

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号制御装置

【特許請求の範囲】

【請求項１】　プログラムを実行するＣＰＵと、該ＣＰＵで実行されるプログラムが格納されたＲＯＭと、該ＣＰＵでのプログラム実行中の作業領域として使用されるＲＡＭと、外部機器との間のデータの送受信を担うＩ／Ｏ部と、暗号化されたデータの復号化および平文のデータの暗号化を担う暗号部とが１つの半導体素子上に形成されてなることを特徴とする暗号制御装置。

【請求項２】　前記ＲＡＭが、暗号化されたデータを復号化するための秘密鍵を格納してなるものであり、

前記ＲＯＭが、この暗号制御装置を使用する正当な権原を有する者を特定するデータを格納してなるものであって、

この暗号制御装置は、外部からデータが送信されてくるのを待つ待機モードと、動作が可能な動作可能モードとを有し、待機モードにあるときに外部から送信されてきた暗号化されたデータを前記ＲＡＭに格納されている秘密鍵で復号化して平文のデータを生成し、該平文のデータと前記ＲＯＭに格納されてなるデータとを照合し、これらのデータが符合するか否かに応じて、それぞれ、動作可能モードに移行し、あるいは待機モードに戻るモード切換手段を有することを特徴とする請求項１記載の暗号制御装置。

【請求項３】　前記ＲＯＭは、前記動作可能モードで実行される複数のメインプログラムを格納してなるものであり、

この暗号制御装置は、前記待機モードにあるときに外部から送信されてきたデータに基づいて、前記動作可能モードで動作させる、前記複数のメインプログラムのうちのいずれか１つのメインプログラムを選択するメインプログラム選択手段を有することを特徴とする請求項２記載の暗号制御装置。

【請求項４】　前記１つの半導体素子がさらに、この暗号制御装置との間で送受信されるデータに基づく情報処理を行なう外部の情報処理装置との間のデータの送受信を担うとともにデータを送信してきた者が正当な権原を有するものであるか否かを認証する認証部を搭載してなるものであることを特徴とする請求項

１記載の暗号制御装置。

【請求項５】　データの暗号化、復号化に用いる鍵を生成する鍵生成手段を有し、この暗号制御装置は、該鍵生成手段で生成された鍵を用いてデータの暗号化および復号化を行なうものであることを特徴とする請求項１記載の暗号制御装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データの暗号化や復号化を担う暗号制御装置に関する。

【０００２】

【従来の技術】

近年の通信技術の発達により、電子マネー等、金券と同等の価値を持つデータが行き交うようになってきており、データの不正な漏洩やデータの改ざんをどのように防止するかが極めて重要になってきている。

【０００３】

このようなデータの安全対策の１つとして、データを暗号化して送り、受信側で受け取ったデータを復号化するという、データの暗号化、復号化という手法が用いられている。このデータの暗号化や復号化には、従来、パーソナルコンピュータ（以下、ＰＣと略記することがある）等の汎用の情報処理装置が使用されている。

【０００４】

また、電子マネー等を取り扱うシステムの典型例として近年ＩＣカードを用いるシステムが注目されているが、ＩＣカードをアクセスするＩＣカードリーダライタ等の周辺機を制御するＩ／Ｏ制御装置としては、従来、複数の半導体素子からなるＩ／Ｏ制御装置が使用されている。

【０００５】

【発明が解決しようとする課題】

汎用の情報処理装置を使用して暗号、復号演算を行なう場合、暗号、復号のアルゴリズムやその暗号、復号に用いる鍵の秘匿が難しく、それらのアルゴリズム

や鍵が不正に漏洩し、データの改ざん等を許すという結果をもらすおそれがある。

【０００６】

また、ＩＣカードリーダライタ等の周辺機を制御するＩ／Ｏ制御装置は、従来、複数の半導体素子で構成されているため、それらの半導体素子間をつなぐアドレスバスやデータバス上にＩ／Ｏ制御の途中経過の情報が出力されることになり、その情報が不正に盗まれるおそれがある。

【０００７】

このように従来は、まだまだデータの安全性に問題があり、その安全性を一層向上させることが求められている。

【０００８】

本発明は、上記事情に鑑み、データの安全性が一層向上した暗号制御装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】

上記的を達成する本発明の暗号制御装置は、プログラムを実行するＣＰＵと、そのＣＰＵで実行されるプログラムが格納されたＲＯＭと、そのＣＰＵでのプログラム実行中の作業領域として使用されるＲＡＭと、外部機器との間のデータの送受信を担うＩ／Ｏ部と、暗号化されたデータの復号化および平文のデータの暗号化を担う暗号部とが１つの半導体素子上に形成されてなることを特徴とする。

【００１０】

本発明の暗号制御装置は、上記の各要素が１つの半導体素子上に搭載されているため、アドレスバスやデータバス上の情報を外部に出力する必要がなく、暗号化、復号化の処理の推測が困難である。

【００１１】

ここで、上記本発明の暗号制御装置は、

上記ＲＡＭが、暗号化されたデータを復号化するための秘密鍵を格納してなるものであり、

上記ＲＯＭが、この暗号制御装置を使用する正当な権原を有する者を特定する

データを格納してなるものであって、

この暗号制御装置は、外部からデータが送信されてくるのを待つ待機モードと、動作が可能な動作可能モードとを有し、待機モードにあるときに外部から送信されてきた暗号化されたデータを上記ＲＡＭに格納されている秘密鍵で復号化して平文のデータを生成し、その平文のデータと上記ＲＯＭに格納されてなるデータとを照合し、これらのデータが符合するか否かに応じて、それぞれ、動作可能モードに移行し、あるいは待機モードに戻るモード切換手段を有することが好ましい。

【００１２】

このような照合を行なうことによって不正なアクセスを防止することができ、また、特に動作する必要のないときは待機モードにあって不必要な電力消費を抑えることができる。

【００１３】

また、この場合に、上記ＲＯＭは、上記動作可能モードで実行される複数のメインプログラムを格納してなるものであり、

この暗号制御装置は、上記待機モードにあるときに外部から送信されてきたデータに基づいて、上記動作可能モードで動作させる、上記複数のメインプログラムのうちのいずれか１つのメインプログラムを選択するメインプログラム選択手段を有することが好ましい。

【００１４】

このように複数のメインプログラムをＲＯＭ内に格納しておくことにより、この暗号制御装置を様々の用途に適用することができ、また動作可能なメインプログラムを待機モードから動作可能モードに移るときに１つだけ選択することにより、複数のメインプログラムどうしの干渉を避け、データの安全性、処理の確実性が保たれる。

【００１５】

また、上記本発明の暗号制御装置において、上記１つの半導体素子がさらに、この暗号制御装置との間で送受信されるデータに基づく情報処理を行なう外部の情報処理装置との間のデータの送受信を担うとともにデータを送信してきた者が

正当な権原を有するものであるか否かを認証する認証部を搭載してなるものであることが好ましい。

【００１６】

１つの半導体素子内にさらに上記のような認証部を搭載すると、認証により外部の情報処理装置との間で送受信されるデータの安全性が保たれる。また、専用の認証部を備えることにより、ＣＰＵでのソフトウェア動作による認証と比べ認証処理の高速化が図られる。

【００１７】

また、本発明において、データの暗号化、復号化に用いる鍵を生成する鍵生成手段を有し、この暗号制御装置は、その鍵生成手段で生成された鍵を用いてデータの暗号化および復号化を行なうものであることが好ましく、この場合に上記鍵生成手段は、秘密鍵と公開鍵とを生成し、公開鍵のみ外部に送信し、秘密鍵は上記ＲＡＭに格納するものであることことが好ましい。

【００１８】

こうすることにより、秘密鍵の秘守性、安全性が保たれ、データの不正な解読が一層困難となる。

【００１９】

また、上記の認証部を備えた構成において、

上記ＲＡＭが、暗号化されたデータを復号化するための秘密鍵を格納してなるものであり、

上記ＲＯＭが、この暗号制御装置を使用する正当な権原を有する者を特定するデータを格納してなるものであって、

上記認証部で受信された暗号化されたデータを上記ＲＡＭに格納されている秘密鍵で復号化して平文のデータを生成し、その平文のデータと上記ＲＯＭに格納されてなるデータとを照合し、これらのデータが符合した場合に限り、上記Ｉ／Ｏ部を動作可能とするＩ／Ｏ部制御手段を有することが好ましく、

この場合に、上記１つの半導体素子が、上記Ｉ／Ｏ部を複数搭載してなるものであって、上記Ｉ／Ｏ部制御手段は、上記認証部で受信されたデータに基づいて、そのデータに応じたＩ／Ｏ部のみ動作可能とするものであることも好ましい形

態であり、

あるいは、上記Ｉ／Ｏ部は、複数のセキュリティレベルのうちの任意のセキュリティレベルの設定が自在なものであり、上記Ｉ／Ｏ部制御手段は、上記認証部で受信されたデータに基づいて、上記Ｉ／Ｏ部を、そのデータに応じたセキュリティレベルに設定するものであることも好ましい形態である。

【００２０】

このような照合を行なうことによって不正なアクセスを防止することができる。また、必要な場合のみＩ／Ｏ部を動作可能とすることが一層の安全性を確保する上で有用であるとともに省電力化を図ることもできる。さらに、上記のようにセキュリティレベルを制御することで、不必要のアクセスの防止を図り、安全性を一層向上させることができる。

【００２１】

また、上記の認証部を備えた構成において、その認証部は、外部の情報処理装置との間のデータの送受信を、モデムを介して行なうものであることも好ましい形態である。

【００２２】

この場合、離れた場所から暗号制御装置の動作を開始させることができる。

【００２３】

さらに、本発明の暗号制御装置において、異常の検知を受けて、上記ＲＡＭに格納されているデータを破壊するデータ破壊手段を有することが好ましい。

【００２４】

こうすることにより鍵が不正な侵入者に渡るのを防止することができる。

【００２５】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

【００２６】

図１は、本発明の暗号制御装置の第１実施形態を示すブロック図である。

【００２７】

この暗号制御装置１０Ａは、１つの半導体素子１００Ａ内に形成されており、

この暗号制御装置１０Ａは、プログラムを実行するＣＰＵ１１Ａ、ＣＰＵ１１Ａでのプログラム実行中の作業領域として使用されるＲＡＭ１２Ａ、ＣＰＵ１１Ａで実行されるプログラムが格納されたＲＯＭ１３Ａ、外部機器（ここではＩＣカードリーダライタ（ＩＣカードＲ／Ｗ）２００）との間でデータを送受信するＩ／Ｏ部１４Ａ，および、暗号化されたデータの復号化や平文のデータの暗号化を担う暗号部１５Ａから構成されている。この暗号制御装置１０Ａを構成する各要素は、内部バス２０Ａで相互に接続されている。

【００２８】

ＲＯＭ１３Ａには暗号処理アルゴリズムやＩ／Ｏ部１４Ａを制御するプログラムなどが含まれている。

【００２９】

また、ＩＣカードＲ／Ｗ２００とＩ／Ｏ部１４Ａとの間で送受信されるデータには、ＩＣカードＲ／Ｗ２００を制御する制御データ、およびＩＣカードから読み出した暗号データがある。ＩＣカードから読み出されるデータはそのＩＣカードの機能によって暗号化されてからそのＩＣカードから読み出され、ＩＣカードＲ／Ｗ２００から暗号制御装置１０Ａに送られる。暗号制御装置１０Ａに送られた暗号データはその暗号制御装置１０Ａの暗号部１５Ａによって復号化される。一方、暗号制御装置１０Ａ内で生成された、ＩＣカードへの送信用のデータは、その暗号制御装置１０Ａの暗号部１５Ａによって暗号化され、Ｉ／Ｏ部１４Ａを経由してＩＣカードＲ／Ｗ２００に送られ、そのＩＣカードＲ／Ｗ２００に挿入されているＩＣカードに書込まれる。ＩＣカード内ではそのＩＣカードの機能によってその暗号データが復号化される。

【００３０】

このような構成を採ることで、暗号部１５ＡとＲＡＭ１２Ａ，ＲＯＭ１３Ａとの間でやりとりされるデータは一切外部に漏れず、セキュリティの高い暗号制御装置が構築される。

【００３１】

図２は、本発明の暗号制御装置の第２実施形態を示すブロック図、図３は、図２に示す第２実施形態における動作フローチャートである。

【００３２】

この暗号制御装置１０Ｂは、１つの半導体素子１００Ｂ内に形成されている。この暗号制御装置１０Ｂは、ＣＰＵ１１Ｂ、ＲＡＭ１２Ｂ、ＲＯＭ１３Ｂ、暗号部１５Ｂ、およびインタフェース部１６Ｂから構成されている。これらのうち、ＣＰＵ１１Ｂ、ＲＡＭ１２Ｂ、ＲＯＭ１３Ｂ、および暗号部１５Ｂは、図１に示す第１実施形態の暗号制御装置１０Ａの、ＣＰＵ１１Ａ、ＲＡＭ１２Ａ、ＲＯＭ１３Ａ、および暗号部１５Ａとそれぞれ同じ要素であり、重複説明は省略する。

【００３３】

また、インタフェース部１６Ｂは、図１に示す暗号制御装置１０ＡのＩ／Ｏ部１４Ａに相当する構成要素であるが、図１のＩ／Ｏ部１４Ａは、ＩＣカードＲ／Ｗ２００との間のデータ送受信に適合したものであるのに対し、この図２に示すインタフェース部１６Ｂは、パーソナルコンピュータ（ＰＣ）３００のＩＳＡバスに接続され、ＰＣ３００との間でＩＳＡバスを介してデータの送受信を行なうのに適合した構成となっている。

【００３４】

図３に示す動作フローは、暗号制御装置１０Ｂに電源が投入されたパワーオン（ＰＯＮ）時に起動されるものである。パワーオンで図３のスタートアップルーチンが起動されると、先ず暗号制御装置１０Ｂの最小限の初期化処理が行なわれ（ステップａ１）、ＰＣ３００からの情報入力待機状態となる（ステップａ２）。この待機状態は、ＰＣ３００からの情報が入力されたときに入力されたことを検知する部分のみ動作し、他の部分は動作しない状態にあり、電力の消費が抑えられている。

【００３５】

ＰＣ３００から送信されてくる情報は暗号化されており、ＰＣ３００から送信されてきた情報を受け取るとその情報の復号処理が行なわれる（ステップａ３）。この復号処理は、ＲＡＭ１２Ｂにあらかじめ格納されている秘密鍵を用いて行なわれる。この段階では暗号部１５Ｂは未だ動作不能状態のままになっており、したがってこのときは暗号部１５Ｂは使用されず、ＲＯＭ１３Ｂに格納されているプログラムによりソフトウェア上で復号処理が行なわれる。

【００３６】

この待機状態においてＰＣ３００から入力される情報にはＩＤやパスワードが含まれており、復号された情報と、あらかじめＲＯＭ１３Ｂに格納されている情報とを照合することにより、この暗号制御装置１０Ｂを使用する正当な権原を有する者から受け取った情報であるか否かの情報確認が行なわれ（ステップａ４）、正当な権原を有する者からの情報ではないと判定されるときは、ステップａ２に戻り、ＰＣからの情報入力待機状態に戻る。

【００３７】

一方、ステップａ４で、正当な権原を有する者からの情報であると判定されたときは、暗号制御装置１０Ｂの各部の初期化設定処理を行ない（ステップａ５）、メインルーチンコールを行なう（ステップａ６）。その後、メインルーチンが実行される（ステップａ７）。

【００３８】

このように、本実施形態の暗号制御装置は、ＰＣからの要請があるまでは待機状態にあり、無駄な電力消費が抑制されている。

【００３９】

図４は、本発明の暗号制御装置の第３実施形態における、ＲＯＭ内部のプログラムの構造を示した模式図である。

【００４０】

この第３実施形態の暗号制御装置の構成自体は、図２に示すものと同じであり、図２を参照することとし、ここでの重複した図面の提示は省略する。

【００４１】

ＲＯＭ１３Ｂに格納されたプログラムは、スタートアップルーチンと、メインルーチン振分けルーチンと、３つのメインルーチンＡ，Ｂ，Ｃとから構成されている。各メインルーチンＡ，Ｂ，Ｃは、それぞれ対応した情報Ａ，Ｂ，Ｃについてのみ参照することができる。メインルーチンＡ，Ｂ，Ｃは、暗号、復号の制御アルゴリズムが相互に異なる一つの暗号制御装置についてタイプの異なる使い方を可能としている。

【００４２】

図５は、図４にプログラム構造を示す第３実施形態における動作フローを示すフローチャートである。

【００４３】

図５に示す動作フローは、図３に示す動作フローの場合と同様、暗号制御装置１０Ｂに電源が投入されたパワーオン（ＰＯＮ）時に起動されるものであり、このパワーオンでは、図４プログラム構造中スタートアップルーチンが起動される。

【００４４】

この図５に示す動作フローにおけるステップｂ１～ｂ５は、それぞれ図３に示す動作フローのステップａ１～ａ５とそれぞれ同一であり、重複説明は省略する。

【００４５】

ステップｂ６では、ステップｂ２で受け取りステップｂ３で復号処理の行なわれた情報に基づいて３つのメインルーチンＡ，Ｂ，Ｃのうちのいずれのメインルーチンを動作させるかが決定され、決定されたメインルーチンについて（ステップｂ７，ｂ８）、内部の初期設定（ステップｂ９，ｂ１０又はｂ１１）およびメインプログラムの実行（ステップｂ１２，ｂ１３又はｂ１４）が行なわれる。

【００４６】

このように、ＲＯＭ内に複数のメインプログラムを格納しておき、待機状態から立ち上がるときに選択的にいずれか１つのメインプログラムのみ動作可能とすることで、様々な用途に適合させることができるとともに、メインプログラムどうしの干渉を避け、データの安全性、処理の確実性が保たれる。

【００４７】

図６は、本発明の暗号制御装置の第４実施形態を示すブロック図である。

【００４８】

この暗号制御装置１０Ｃは、１つの半導体素子１００Ｃ内に形成されたものであり、ＣＰＵ１１Ｃ、ＲＡＭ１２Ｃ、ＲＯＭ１３Ｃ、Ｉ／Ｏ部１４Ｃ、および暗号部１５Ｃは、図１に示す第１実施形態の暗号制御装置１０Ａの、対応する各要素とそれぞれ同一であり、重複説明は省略する。尚、この図６では、ＲＡＭ１２

Ｃに鍵が格納されていることが模式的に明示されている。

【００４９】

また、図６の暗号制御装置１０Ｃを構成する認証部１６Ｃは、ＰＣ３００と接続されてそのＰＣ３００との間でシリアルデータの送受信を行なうインタフェースであるとともに、データを送信してきた者が正当な権原を有する者であるか否かを認証するという役割りを担っている。

【００５０】

図７は、ＰＣ３００から暗号制御装置１０Ｃに向けて送信される認証データのデータ構造を示す図である。

【００５１】

ＰＣ３００から暗号制御装置１０Ｃへは、そのＰＣ３００のユーザを特定するＩＤおよびパスワードと、Ｉ／Ｏ部１４Ｃを制御するための情報であるＩ／Ｏ情報が含まれており、この認証データは、暗号制御装置１０Ｃの暗号部１５Ｃで前もって作成され認証部１６Ｃを経由して受け取っている公開鍵（以下に説明する図８に示す公開鍵０）で暗号化されたものである。

【００５２】

図８は、ＰＣ３００と暗号制御装置１０Ｃとの間での認証の手順を示した図である。

【００５３】

先ず、暗号制御装置では前もって秘密鍵１と公開鍵０を生成し公開鍵０がＰＣに渡されている。秘密鍵は、暗号制御装置１０ＣのＲＡＭ１２Ｃに格納しておき、決して外部には出さないようにしておく。この公開鍵０を用いて暗号化されたデータは、秘密鍵１を用いてのみ復号化することができる。

【００５４】

ＰＣでは、暗号制御装置との間でデータの送受信を行なうとしたとき、先ず、図７に示すデータ形式の認証データを作成し、その認証データを、あらかじめ暗号制御装置から受け取っている公開鍵０で暗号化して暗号制御装置に送る。

【００５５】

暗号制御装置は、この暗号化された認証データを受け取ると、ＲＡＭ１２Ｃに

あらかじめ格納しておいた秘密鍵１を用いてその認証データを復号化して平文の認証データを生成する。尚、この認証データの受信の際は、この暗号制御装置は待機状態にあり必要最小限の要素のみ動作し、例えば図６に示すＩ／Ｏ部１４Ｃや復号部１５Ｃは非動作状態にあり、したがってこの認証データの復号化はＲＯＭ１３Ｃに格納されている復号化プログラムによりソフトウェア的に行なわれる。

【００５６】

暗号制御装置では、この復号化された認証データを秘密鍵１で復号化して平文の認証データを生成した後、その生成した平文の認証データがＲＯＭ１３にあらかじめ格納しておいた照合用の認証データと照合される。この照合により双方の認証データが一致したときは、以下に説明する次のステップに移り、不一致のときはＰＣ３００から次のデータの受信を待機する待機状態に戻る。

【００５７】

双方の認証データが一致すると、今度は、ＲＯＭ１３Ｃ内部のアルゴリズムで、乱数Ａと、秘密鍵２と、２つの公開鍵１，２とが生成され、ＲＯＭ内のアルゴリズムで乱数Ａと公開鍵２が公開鍵１で暗号化され、その公開鍵１で暗号化された乱数Ａと公開鍵２がＰＣに送信されるとともに、公開鍵１自身もＰＣに送信される。生成された秘密鍵２は、ＲＡＭ１２Ｃに格納される。また乱数Ａおよび公開鍵２もＲＡＭ１２Ｃに格納される。

【００５８】

ＰＣ３００は、暗号制御装置から公開鍵１と、その公開鍵１で暗号化された乱数Ａと公開鍵２を受け取ると、暗号化された乱数Ａと公開鍵２を公開鍵１で復号して平文の乱数Ａと公開鍵２を取り出し、さらに乱数Ｂを生成し、公開鍵１による復号により取り出した乱数Ａと新たに発生させた乱数Ｂを、上記のようにして取り出した公開鍵２で暗号化して暗号制御装置に送信する。この乱数ＢはＰＣ内にも記憶しておく。

【００５９】

暗号制御装置では、それを受信すると、その受信データをＲＡＭ１２Ｃに記憶しておいた秘密鍵２で復号して乱数Ａと乱数Ｂを取り出し、この取り出した乱数

Ａと乱数Ｂのうちの乱数Ａと、先に発生させてＲＡＭ１２Ｃに格納しておいた乱数Ａとが照合され、それらが一致した場合に、暗号制御装置は、そこに接続されたＰＣが暗号制御装置をアクセスする正当な権原を有する者であると認証する。不一致のときは、図８には示されていないがＰＣに向けて不一致であった旨連絡して待機状態に戻る。

【００６０】

暗号制御装置で受信して復号化した乱数ＡとＲＡＭ１２Ｃに格納しておいた乱数Ａが一致すると、今度は公開鍵３を生成し、ＰＣ３００から送信されて復号化された乱数Ｂと公開鍵３を、ＲＡＭ１２Ｃに格納しておいた公開鍵２で暗号化しＰＣに向けて送信する。公開鍵３はＲＡＭ１２Ｃにも格納される。

【００６１】

ここで、公開鍵３は、その公開鍵３で暗号化したデータをその公開鍵３自身で復号化することのできる鍵である。

【００６２】

公開鍵２で暗号化された乱数Ｂと公開鍵３を受信したＰＣでは、受信したデータを公開鍵２で復号し、その復号化されたデータに含まれる乱数Ｂと公開鍵３のうちの乱数Ｂと、この乱数ＢはＰＣが自分で発生させたものであって、その発生させて記憶しておいた乱数Ｂとが照合され、それらが一致しているときは、自分が送受信している相手が、確かに自分がデータを送受信しようとしていた暗号制御装置である旨、認証する。

【００６３】

これまでの間の、暗号制御装置におけるデータの復号化、暗号化は、全てＲＯＭ１３Ｃのアルゴリズムによりソフトウェア的に行なわれる。

【００６４】

また、上記のようにして、そこに接続されたＰＣが暗号制御装置を正当にアクセスする権原を有する者であることが確認された後、暗号制御装置では暗号部１５Ｃが動作可能状態とり、これ以降の暗号化、復号化は、暗号部１５Ｃにより、ＲＯＭ内のアルゴリズムを用いてソフトウェア的に行なうよりも高速に行なわれる。

【００６５】

また、図７に示す認証データのＩ／Ｏ情報に応じて、そのＩ／Ｏ情報がＩ／Ｏ部１４Ｃを動作可能状態に移行させることを指示していたときはＩ／Ｏ部１４Ｃも動作可能状態となり、そのＩ／Ｏ情報がＩ／Ｏ部１４Ｃを動作可能とする必要のないことを指示していたときはＩ／Ｏ部１４Ｃは非動作状態にとどまる。こうすることによりＩ／Ｏ部１４Ｃを動作させる必要のないときはＩ／Ｏ部１４Ｃにおける電力消費が抑えられるとともに、暗号制御装置内部と外部との通信路を接続しておく機会の減少化を図り、一層の安全性が確保される。

【００６６】

上記のようにしてＰＣと暗号制御装置との間での相互の認証が終了した後、ＰＣから暗号制御装置に向けてコマンドが送信され、暗号制御装置からはＰＣに向けてそのコマンドに対するレスポンスが送信されるが、ＰＣから暗号制御装置に送信されるコマンドはＰＣ側で公開鍵３で暗号化されて送信され、それを受け取った暗号制御装置側では、その暗号部１５Ｃにより、ＲＡＭ１２Ｃに格納しておいた公開鍵３を用いて復号化され、そのコマンドが実行される。

【００６７】

そのコマンドが実行された結果得られたコマンド結果（レスポンス）は暗号制御装置の暗号部１５Ｃで公開鍵３で暗号化されてＰＣに送信され、その暗号化されたレスポンスを受け取ったＰＣ側では、そのレスポンスが公開鍵３で復号化されてレスポンスが取り出される。

【００６８】

以後、必要に応じてＰＣと暗号制御装置との間でこれと同様な通信が行なわれる。

【００６９】

ここで、上記のように、暗号制御装置には鍵生成手段が備えられており、この暗号制御装置では、その暗号制御装置自身で生成した鍵のみを用いて、復号化、暗号化が行なわれており、また秘密鍵は一切外出には出さないようになっている。また、認証により正当な通信相手ではないと判定されると暗号制御装置は待機状態に戻ってしまい動作しなくなり、また実質のデータ通信は認証により正当な

通信相手であることが確認された後に初めて行なわれる。このような構成により、データの秘密性、安全性が保たれ、データの不正な解読はほとんど不可能となる。

【００７０】

図９は、本発明の暗号制御装置の第５実施形態のブロック図である。図６に示す第４実施形態の暗号制御装置との相違点について説明する。

【００７１】

図９に示す第５実施形態の暗号制御装置には、図６に示す第４実施形態の暗号制御装置のＩ／Ｏ部１４Ｃに相当する、３つのＩ／Ｏ部１４１Ｄ，１４２Ｄ，１４３Ｄ（ＩＣＣ，ＵＡＲＴ１，ＵＡＲＴ２）が備えられている。これら３つのＩ／Ｏ部１４１Ｄ，１４２Ｄ，１４３Ｄを含む暗号制御装置１０Ｄを構成する各要素は１つの半導体素子１００Ｄに搭載されている。各Ｉ／Ｏ部１４１Ｄ，１４２Ｄ，１４３Ｄには、それぞれＩＣカードＲ／Ｗ２００、プリンタ（ＰＲ）４００、および遠隔通信用のモデム（ＭＯＤＥＭ）３００が接続されている。

【００７２】

図９は、図８に示す第５実施形態の暗号制御装置に向けて送信される認証データのデータ構造を示す図である。

【００７３】

この図９に示す認証データには、図７に示す認証データと比べ、コマンド情報が付加されている。

【００７４】

このコマンド情報は、３つのＩ／Ｏ部１４１Ｄ，１４２Ｄ，１４３Ｄのうち、Ｉ／Ｏ情報で指定されるＩ／Ｏ部を動作可能状態とする（Ｏｐｅｎ）か、動作状態から非動作状態に戻す（Ｃｌｏｓｅ）か、あるいは、Ｉ／Ｏ情報で指定されるＩ／Ｏ部を動作可能状態とするとともに他の動作可能状態のＩ／Ｏ部があったときはそれを非動作状態に変更する（Ｃｈａｎｇｅ）かのいずれかのコマンドを示しており、ＰＣからは、この認証データが暗号化されて暗号制御装置に送信され、暗号制御装置では受け取ったデータを復号化して平文の認証データを取り出し図８を参照して説明したようにして認証を行なった後、図９に示す３つのＩ／Ｏ

部１４１Ｄ，１４２Ｄ，１４３Ｄを、その認証データ中のコマンド情報およびＩ／Ｏ情報に従って制御する。

【００７５】

こうすることにより、今回の処理に必要なＩ／Ｏ部以外のＩ／Ｏ部は非動作状態に保たれ、その電力消費が抑えられ、かつ、そのＩ／Ｏ部から出力されるデータが不正に解読されるおそれをなくしている。

【００７６】

さらに、図９に示す３つのＩ／Ｏ部１４１Ｄ，１４２Ｄ，１４３Ｄは、いずれもセキュリティレベルが、非動作状態（アクセス権無し）を含む複数段階に変更できるものであり、それに対応して、コマンド情報には、セキュリティレベルを０から１に変更するＬｅｖｅｌＵｐ１コマンド、セキュリティレベルを１から２に変更するＬｅｖｅｌＵｐ２コマンド、セキュリティレベルを２から３に変更するＬｅｖｅｌＵｐ３コマンド、およびセキュリティレベルを現在のセキュリティレベルから１つダウンさせるＬｅｖｅｌＤｎコマンドを含ませることができる。

【００７７】

図１１は、各セキュリティレベルごとのアクセス権の範囲と、各コマンドとの対応を示した図である。また、表１は、各セキュリティレベルごとのコマンドの作用を示したものである。

【００７８】

【表１】

	Level 1 UP1 ｺﾏﾝﾄﾞ	Level 1 UP2 ｺﾏﾝﾄﾞ	Level 1 UP3 ｺﾏﾝﾄﾞ	Level 1 Dn ｺﾏﾝﾄﾞ
ｾｷｭﾘﾃｨﾚﾍﾞﾙ 0	ｾｷｭﾘﾃｨﾚﾍﾞﾙ 1 へ	ｴﾗｰ	ｴﾗｰ	ｴﾗｰ
ｾｷｭﾘﾃｨﾚﾍﾞﾙ 1	NOP	ｾｷｭﾘﾃｨﾚﾍﾞﾙ 2 へ	ｾｷｭﾘﾃｨﾚﾍﾞﾙ 3 へ	ｾｷｭﾘﾃｨﾚﾍﾞﾙ 0 へ
ｾｷｭﾘﾃｨﾚﾍﾞﾙ 2	ｴﾗｰ	NOP	ｾｷｭﾘﾃｨﾚﾍﾞﾙ 3 へ	ｾｷｭﾘﾃｨﾚﾍﾞﾙ 1 へ
ｾｷｭﾘﾃｨﾚﾍﾞﾙ 3	ｴﾗｰ	ｴﾗｰ	NOP	ｾｷｭﾘﾃｨﾚﾍﾞﾙ 2 へ

【００７９】

このように、複数のセキュリティレベルを設けることにより、不必要なアクセ

スが防止され、安全性が一層向上する。

【００８０】

尚、図９に示す第５実施形態の暗号制御装置では、認証部１６Ｄは、ＰＣ３００との接続部に用いられているが、モデム５００を制御するＩ／Ｏ部１４３Ｄの内部に認証部を備えてもよい。こうすること、モデム５００の先にＰＣ等を接続し、遠隔からこの暗号制御装置を動作させることができる。

【００８１】

図１２は、本発明の暗号制御装置の第６実施形態を示す模式図である。

【００８２】

この図１２の暗号制御装置１０Ｅには、ＳＲＡＭ１２Ｅのみ示されているが、このＳＲＡＭ１２Ｅは、図９に示すＲＡＭ１２Ｄに代わるものであり、図１２には図示省略されているが、図１２に示す暗号制御装置は図９に示す各要素と同じ要素からなり、それらが１つのＬＳＩチップ１００Ｅ上に搭載されている。

【００８３】

この図１２には、ＬＳＩチップ１００Ｅに搭載された暗号制御装置１０Ｅが組み込まれた装置の筐体６００が示されており、この筐体６００内には、商用電源からの電力を暗号制御装置１０ＥのＳＲＡＭ１２Ｅに供給するメイン電源部６０１、バッテリに蓄積された電力をＳＲＡＭ１２Ｅに供給するバッテリ電源部６０２、この筐体６００の分解や解体を検知する攻撃検知センサ６０３、その攻撃検知センサ６０３からの信号を受けて筐体６００が無理にこじ開けられようとしているなどの分解や解体を検出する異常検出器６０４が備えられている。尚、暗号制御装置１０ＥのＳＲＡＭ１２Ｅ以外の各要素へも電力が供給されるが、ここではＳＲＡＭ１２Ｅに注目しているため、他の要素およびそれら他の要素への電力供給経路等は図示省略されている。

【００８４】

ここで、攻撃検知センサ６０３からの信号により異常検出器６０４が筐体６００の分解、解体などの異常を検知すると、その旨をメイン電源部６０１に通知し、メイン電源部６０１はそれを受けてＳＲＡＭ１２Ｅを含む暗号制御装置１０Ｅへの電力供給を強制的に遮断する。また、異常検出器６０４は、バッテリ電源部

６０２から暗号制御装置１０Ｅへの電力供給路を断ち切る。ＳＲＡＭ１２Ｅには、前述したようにして鍵が格納されるが、このよにして電力の供給が断たれるとＳＲＡＭ１２Ｅに格納された鍵やその他のデータは破壊されることになる。したがって不正に分解や解体を行なって鍵やその他のデータを不正に盗もうとしても失敗する結果となり、データの不正な漏洩が防止される。

【００８５】

尚、ここでは電力の供給を断つことにより鍵やその他のデータを破壊する例を示したが、この他にも、攻撃検知センサ６０３の信号あるいは異常検出器６０４の検出結果を暗号制御装置１０Ｅに割込信号として入力し、暗号制御装置では、その割込入力を受けてＳＲＡＭ１２Ｅに無意味なデータを上書きをすることなどにより、ソフトウェア的に鍵やデータを破壊してもよい。

【００８６】

以下に、本発明の各種態様を付記する。

【００８７】

（付記１）　プログラムを実行するＣＰＵと、該ＣＰＵで実行されるプログラムが格納されたＲＯＭと、該ＣＰＵでのプログラム実行中の作業領域として使用されるＲＡＭと、外部機器との間のデータの送受信を担うＩ／Ｏ部と、暗号化されたデータの復号化および平文のデータの暗号化を担う暗号部とが１つの半導体素子上に形成されてなることを特徴とする暗号制御装置。

【００８８】

（付記２）　前記ＲＡＭが、暗号化されたデータを復号化するための秘密鍵を格納してなるものであり、

前記ＲＯＭが、この暗号制御装置を使用する正当な権原を有する者を特定するデータを格納してなるものであって、

この暗号制御装置は、外部からデータが送信されてくるのを待つ待機モードと、動作が可能な動作可能モードとを有し、待機モードにあるときに外部から送信されてきた暗号化されたデータを前記ＲＡＭに格納されている秘密鍵で復号化して平文のデータを生成し、該平文のデータと前記ＲＯＭに格納されてなるデータとを照合し、これらのデータが符合するか否かに応じて、それぞれ、動作可能モ

ードに移行し、あるいは待機モードに戻るモード切換手段を有することを特徴とする付記１記載の暗号制御装置。

【００８９】

（付記３）　前記ＲＯＭは、前記動作可能モードで実行される複数のメインプログラムを格納してなるものであり、

この暗号制御装置は、前記待機モードにあるときに外部から送信されてきたデータに基づいて、前記動作可能モードで動作させる、前記複数のメインプログラムのうちのいずれか１つのメインプログラムを選択するメインプログラム選択手段を有することを特徴とする付記２記載の暗号制御装置。

【００９０】

（付記４）　前記１つの半導体素子がさらに、この暗号制御装置との間で送受信されるデータに基づく情報処理を行なう外部の情報処理装置との間のデータの送受信を担うとともにデータを送信してきた者が正当な権原を有するものであるか否かを認証する認証部を搭載してなるものであることを特徴とする付記１記載の暗号制御装置。

【００９１】

（付記５）　データの暗号化、復号化に用いる鍵を生成する鍵生成手段を有し、この暗号制御装置は、該鍵生成手段で生成された鍵を用いてデータの暗号化および復号化を行なうものであることを特徴とする付記１記載の暗号制御装置。

【００９２】

（付記６）　前記鍵生成手段は、秘密鍵と公開鍵とを生成し、公開鍵のみ外部に送信し、秘密鍵は前記ＲＡＭに格納するものであることを特徴とする付記５記載の暗号制御装置。

【００９３】

（付記７）　前記ＲＡＭが、暗号化されたデータを復号化するための秘密鍵を格納してなるものであり、

前記ＲＯＭが、この暗号制御装置を使用する正当な権原を有する者を特定するデータを格納してなるものであって、

前記認証部で受信された暗号化されたデータを前記ＲＡＭに格納されている秘

密鍵で復号化して平文のデータを生成し、該平文のデータと前記ＲＯＭに格納されてなるデータとを照合し、これらのデータが符合した場合に限り、前記Ｉ／Ｏ部を動作可能とするＩ／Ｏ部制御手段を有することを特徴とする付記４記載の暗号制御装置。

【００９４】

（付記８）　前記１つの半導体素子が、前記Ｉ／Ｏ部を複数搭載してなるものであって、

前記Ｉ／Ｏ部制御手段は、前記認証部で受信されたデータに基づいて、該データに応じたＩ／Ｏ部のみ動作可能とするものであることを特徴とする付記７記載の暗号制御装置。

【００９５】

（付記９）　前記Ｉ／Ｏ部は、複数のセキュリティレベルのうちの任意のセキュリティレベルの設定が自在なものであり、

前記Ｉ／Ｏ部制御手段は、前記認証部で受信されたデータに基づいて、前記Ｉ／Ｏ部を、該データに応じたセキュリティレベルに設定するものであることを特徴とする付記７記載の暗号制御装置。

【００９６】

（付記１０）　前記認証部は、外部の情報処理装置との間のデータの送受信を、モデムを介して行なうものであることを特徴とする付記４記載の暗号制御装置。

【００９７】

（付記１１）　異常の検知を受けて、前記ＲＡＭに格納されている鍵を破壊するデータ破壊手段を有することを特徴とする付記１記載の暗号制御装置。

【００９８】

【発明の効果】

以上、説明したように、本発明によれば不正なデータの解読や漏洩が防止されデータの安全性が高度に保たれた暗号制御装置が実現する。

【図面の簡単な説明】

【図１】

本発明の暗号制御装置の第１実施形態を示すブロック図である。

【図２】

本発明の暗号制御装置の第２実施形態を示すブロック図である。

【図３】

図２に示す第２実施形態における動作フローチャートである。

【図４】

本発明の暗号制御装置の第３実施形態における、ＲＯＭ内部のプログラムの構造を示した模式図である。

【図５】

図４にプログラム構造を示す第３実施形態における動作フローを示すフローチャートである。

【図６】

本発明の暗号制御装置の第４実施形態を示すブロック図である。

【図７】

認証データのデータ構造を示す図である。

【図８】

本発明の暗号制御装置の第５実施形態のブロック図である。

【図９】

図８に示す第５実施形態の暗号制御装置に向けて送信される認証データのデータ構造を示す図である。

【図１０】

認証データのデータ構造を示す図である。

【図１１】

各セキュリティレベルごとのアクセス権の範囲と、各コマンドとの対応を示した図である。

【図１２】

本発明の暗号制御装置の第６実施形態を示す模式図である。

【符号の説明】

１０Ａ，１０Ｂ，１０Ｃ，１０Ｄ，１０Ｅ　　暗号制御装置

１１Ａ，１１Ｂ，１１Ｃ，１１Ｄ　ＣＰＵ

１２Ａ，１２Ｂ，１２Ｃ，１２Ｄ　ＲＡＭ

１３Ａ，１３Ｂ，１３Ｃ，１３Ｄ　ＲＯＭ

１４Ａ，１４Ｃ　Ｉ／Ｏ部

１５Ａ，１５Ｂ，１５Ｃ　暗号部

１６Ｂ，１６Ｃ，１６Ｄ　インタフェース部

１４１Ｄ，１４２Ｄ，１４３Ｄ　Ｉ／Ｏ部

２０Ａ，２０Ｂ，２０Ｃ　内部バス

１００Ａ，１００Ｂ，１００Ｃ，１００Ｄ，１００Ｅ　半導体素子

２００　ＩＣカードＲ／Ｗ

３００　パーソナルコンピュータ（ＰＣ）

４００　プリンタ（ＰＲ）

５００　モデム

６００　筐体

６０１　メイン電源部

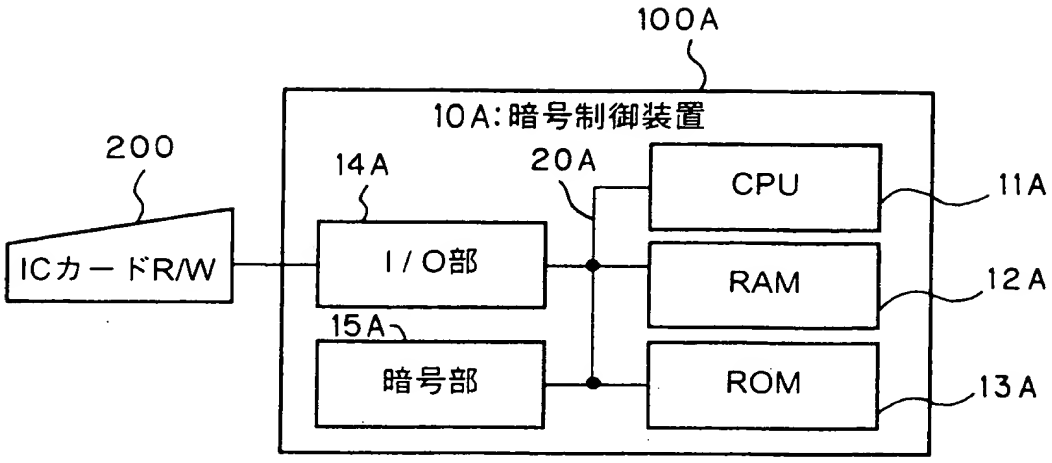
６０２　バッテリ電源部

６０３　攻撃検知センサ

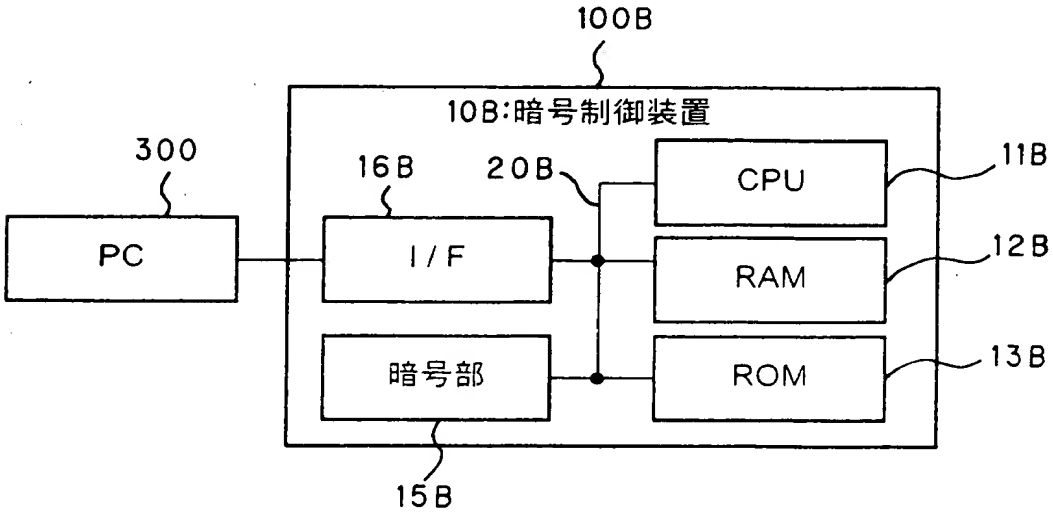
６０４　異常検出器

【書類名】　　図面

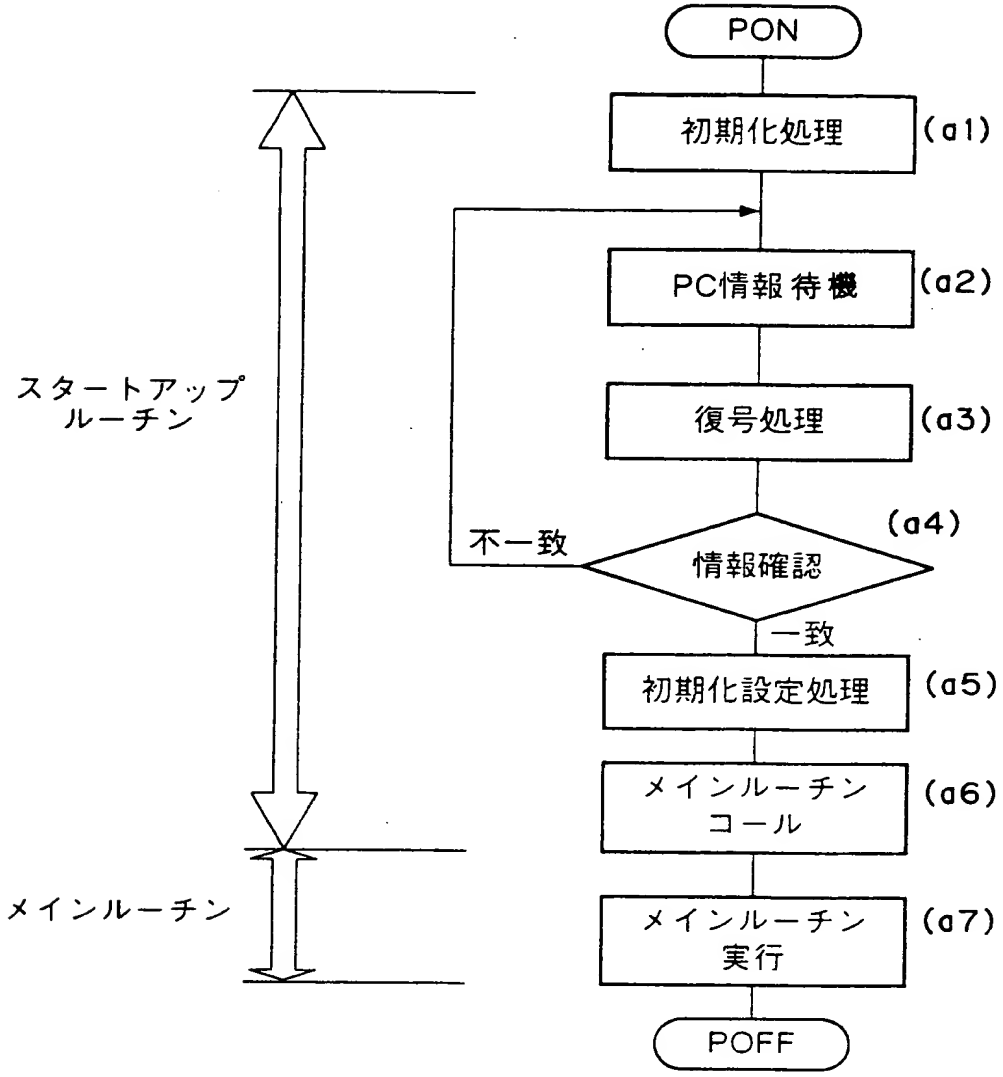
【図１】


100A
10A:暗号制御装置
200
14A
20A
CPU
11A
ICカードR/W
I/O部
RAM
12A
15A
暗号部
ROM
13A

【図２】

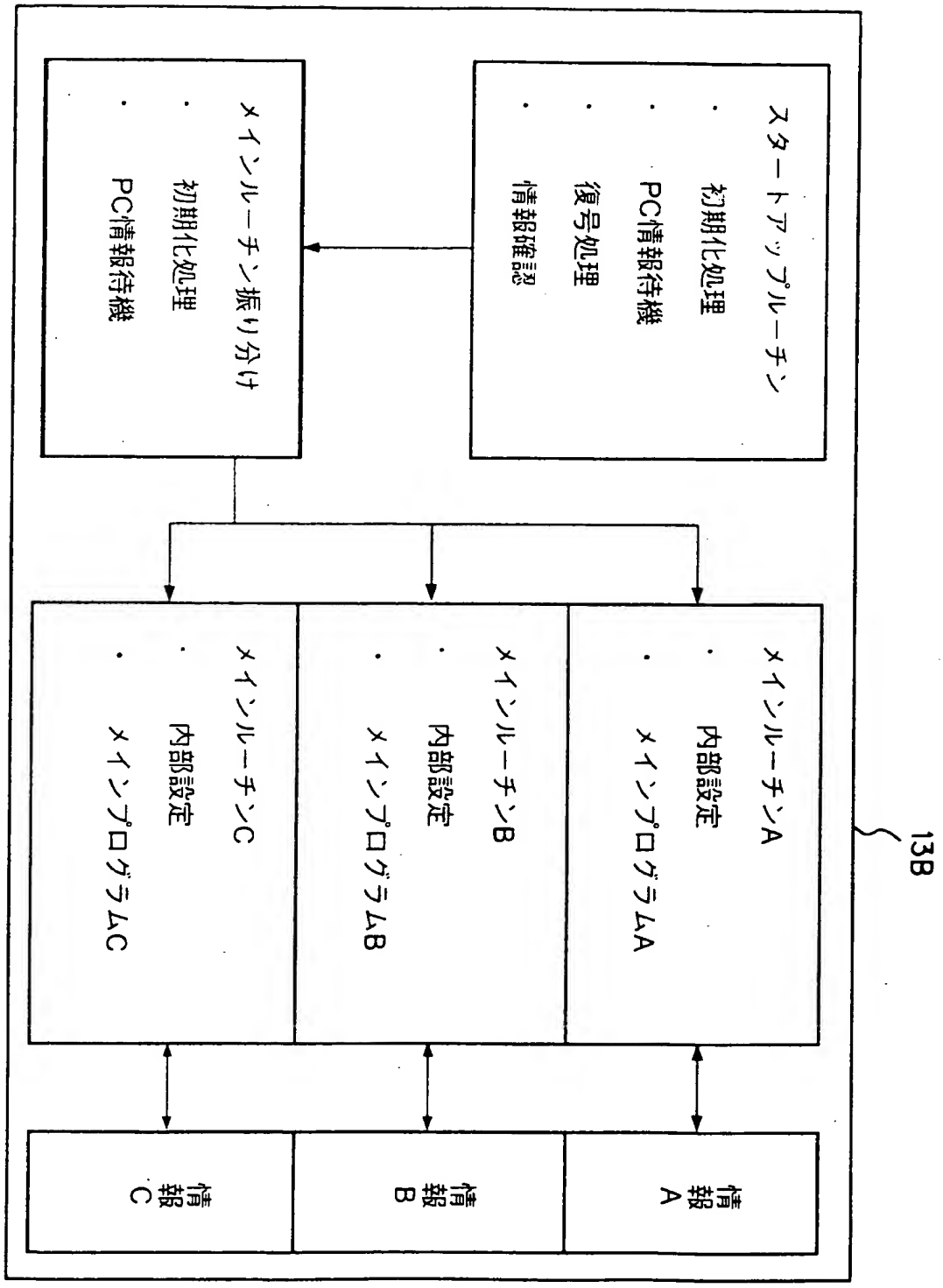

100B
10B:暗号制御装置
300
16B
20B
CPU
11B
PC
I/F
RAM
12B
暗号部
ROM
13B
15B

【図３】

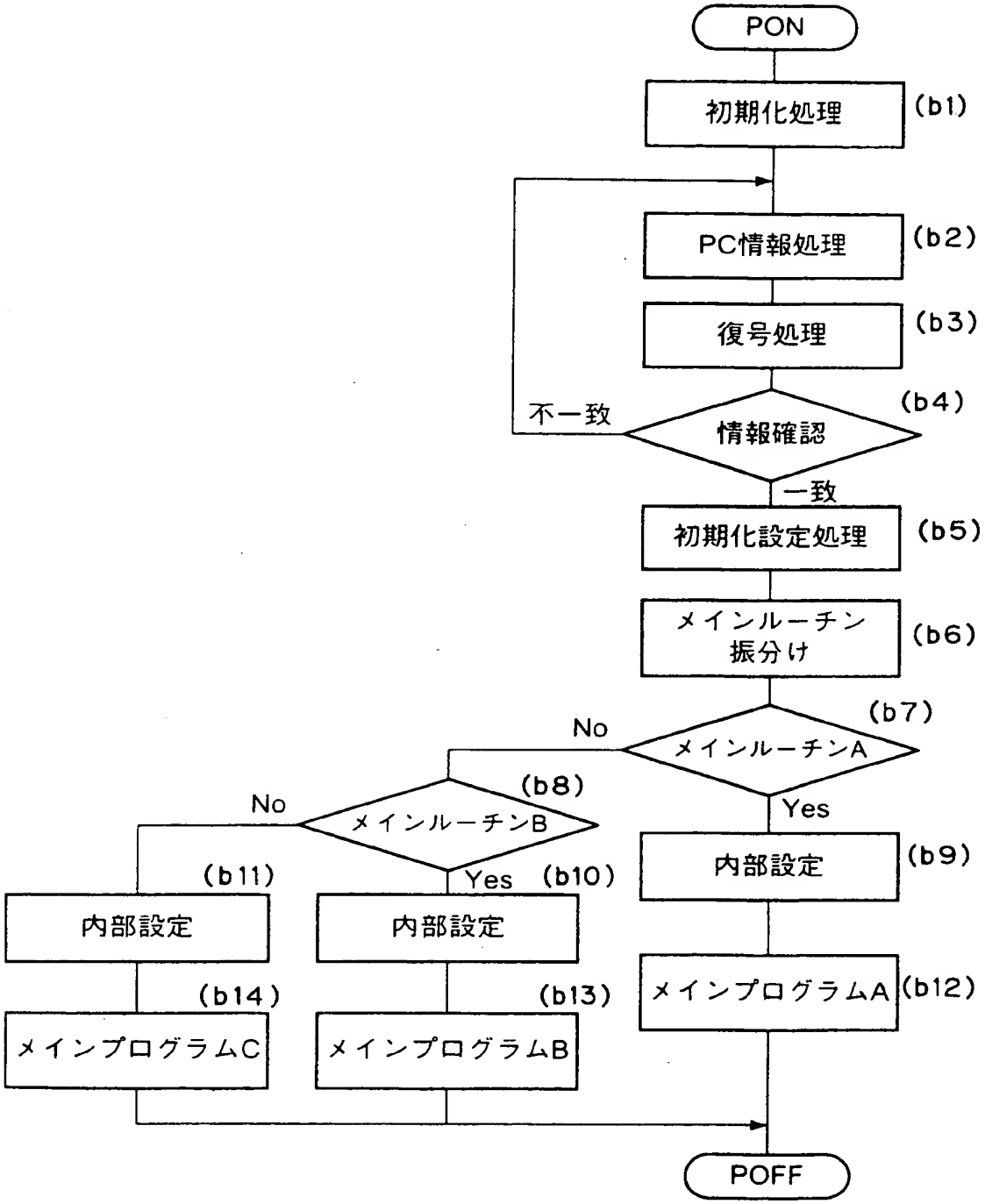


出証特２０００－３０７６９７２

【図４】

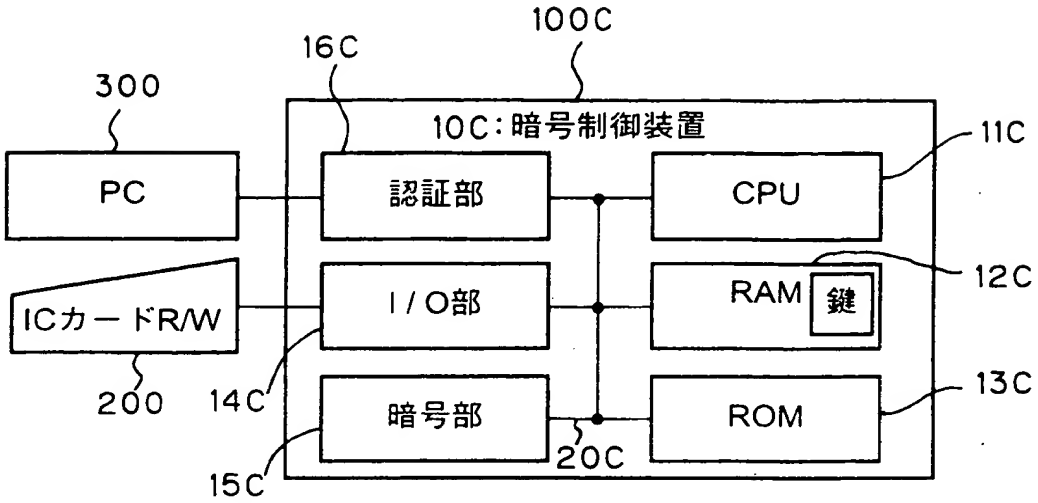

スタートアップルーチン
・ 初期化処理
・ PC情報待機
・ 復号処理
・ 情報確認
メインルーチン振り分け
・ 初期化処理
・ PC情報待機
メインルーチンA
・ 内部設定
・ メインプログラムA
メインルーチンB
・ 内部設定
・ メインプログラムB
メインルーチンC
・ 内部設定
・ メインプログラムC
情報A
情報B
情報C
13B

【図５】

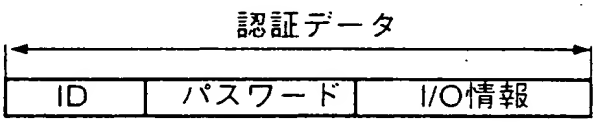


出証特２０００－３０７６９７２

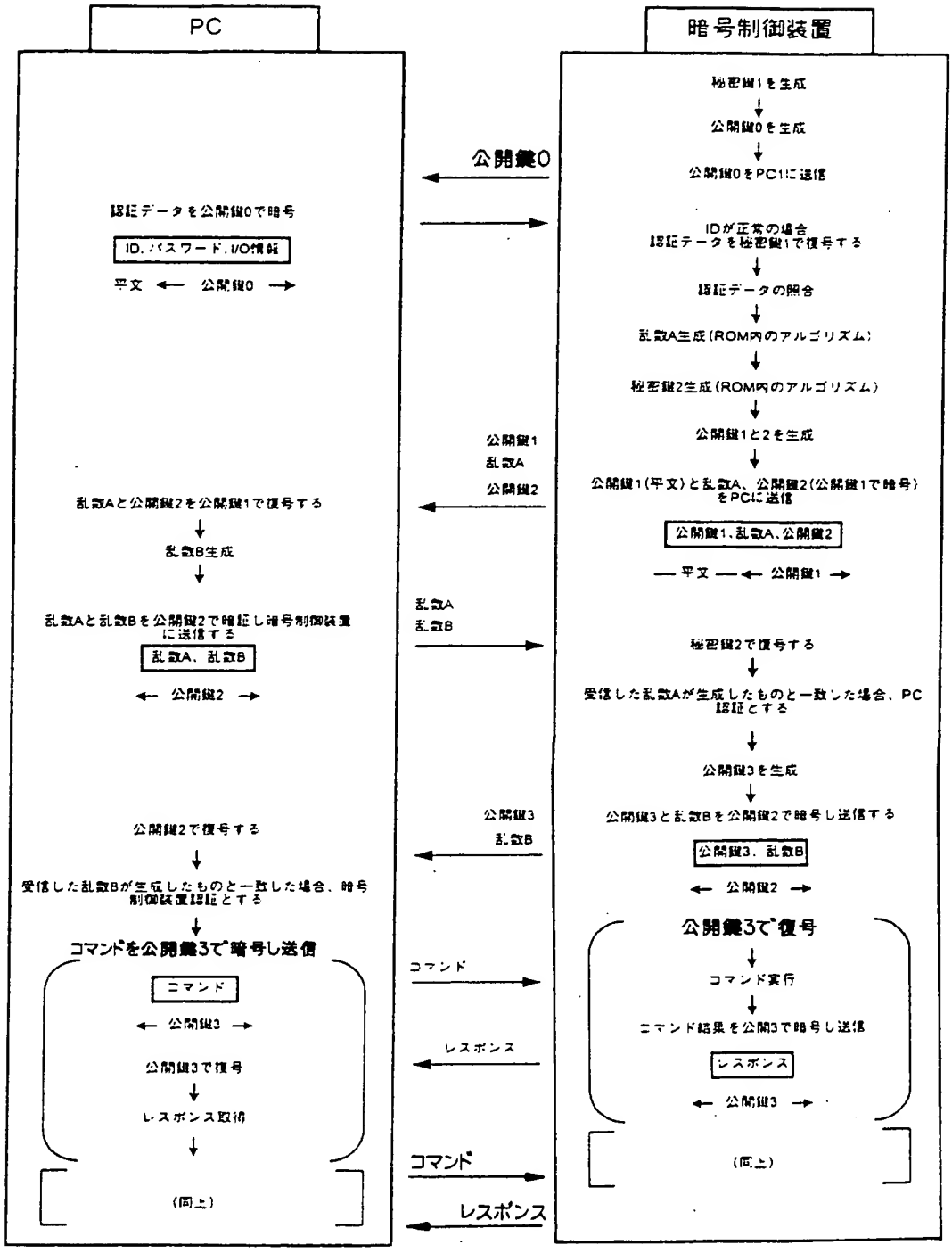
【図６】


100C
16C
300
10C：暗号制御装置
11C
PC
認証部
CPU
12C
RAM
鍵
ICカードR/W
I/O部
200
14C
暗号部
ROM
13C
20C
15C

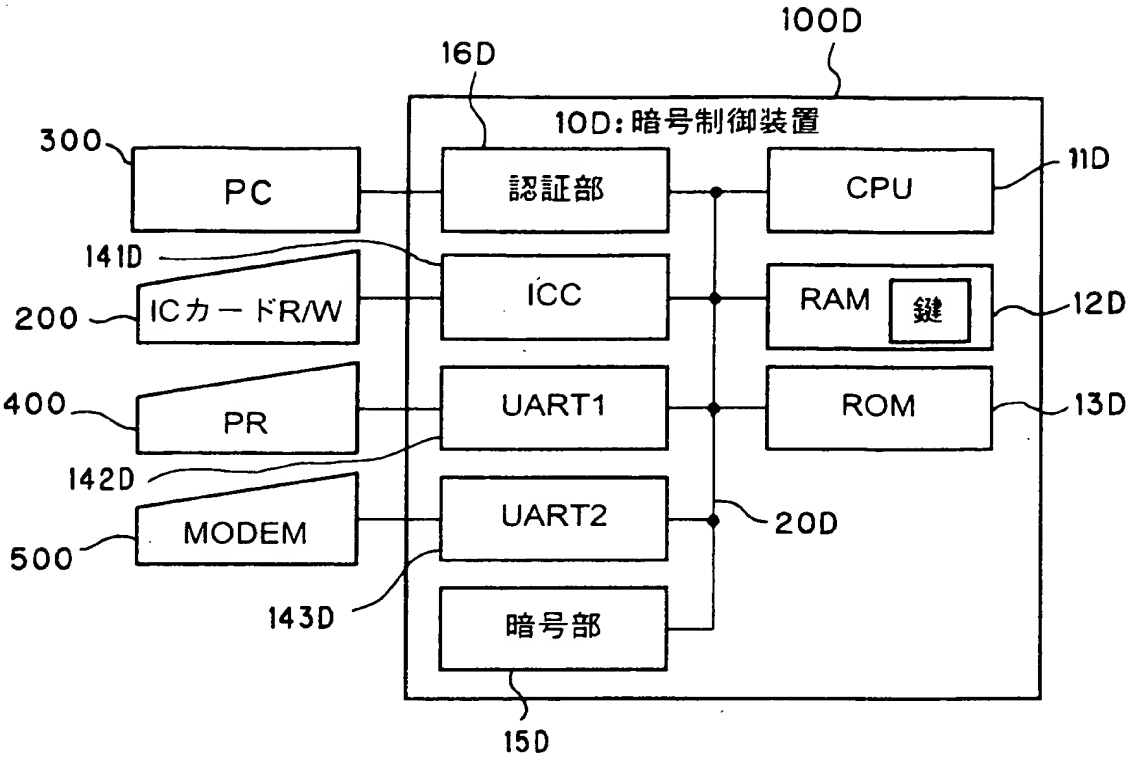
【図７】


認証データ
ID
パスワード
I/O情報

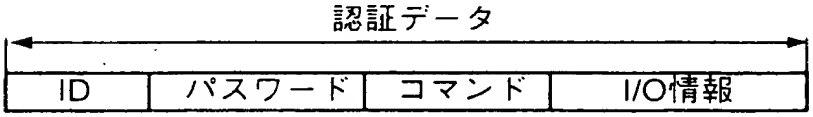
【図８】


PC
暗号制御装置
秘密鍵1を生成
公開鍵0を生成
公開鍵0
公開鍵0をPC1に送信
認証データを公開鍵0で暗号
ID、パスワード、I/O情報
平文 ← 公開鍵0 →
IDが正常の場合
認証データを秘密鍵1で復号する
認証データの照合
乱数A生成(ROM内のアルゴリズム)
秘密鍵2生成(ROM内のアルゴリズム)
公開鍵1と2を生成
公開鍵1
乱数A
公開鍵2
公開鍵1(平文)と乱数A、公開鍵2(公開鍵1で暗号)をPCに送信
乱数Aと公開鍵2を公開鍵1で復号する
乱数B生成
公開鍵1、乱数A、公開鍵2
— 平文 —← 公開鍵1 →
乱数A
乱数B
乱数Aと乱数Bを公開鍵2で暗証し暗号制御装置に送信する
乱数A、乱数B
← 公開鍵2 →
秘密鍵2で復号する
受信した乱数Aが生成したものと一致した場合、PC認証とする
公開鍵3を生成
公開鍵3
乱数B
公開鍵3と乱数Bを公開鍵2で暗号し送信する
公開鍵3、乱数B
← 公開鍵2 →
公開鍵2で復号する
受信した乱数Bが生成したものと一致した場合、暗号制御装置認証とする
コマンドを公開鍵3で暗号し送信
公開鍵3で復号
コマンド
コマンド
← 公開鍵3 →
コマンド実行
コマンド結果を公開3で暗号し送信
レスポンス
レスポンス
← 公開鍵3 →
公開鍵3で復号
レスポンス取得
(同上)
(同上)
コマンド
レスポンス

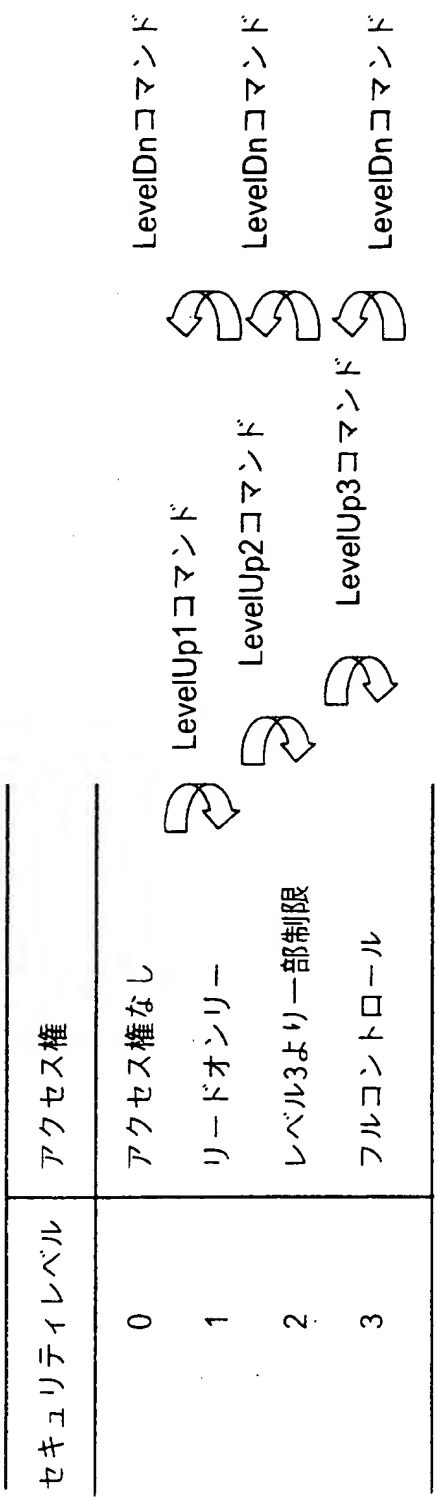
【図９】


100D
16D
10D:暗号制御装置
300
PC
認証部
CPU
11D
141D
ICC
200
ICカードR/W
RAM
鍵
12D
400
PR
UART1
ROM
13D
142D
MODEM
UART2
20D
500
143D
暗号部
15D

【図１０】

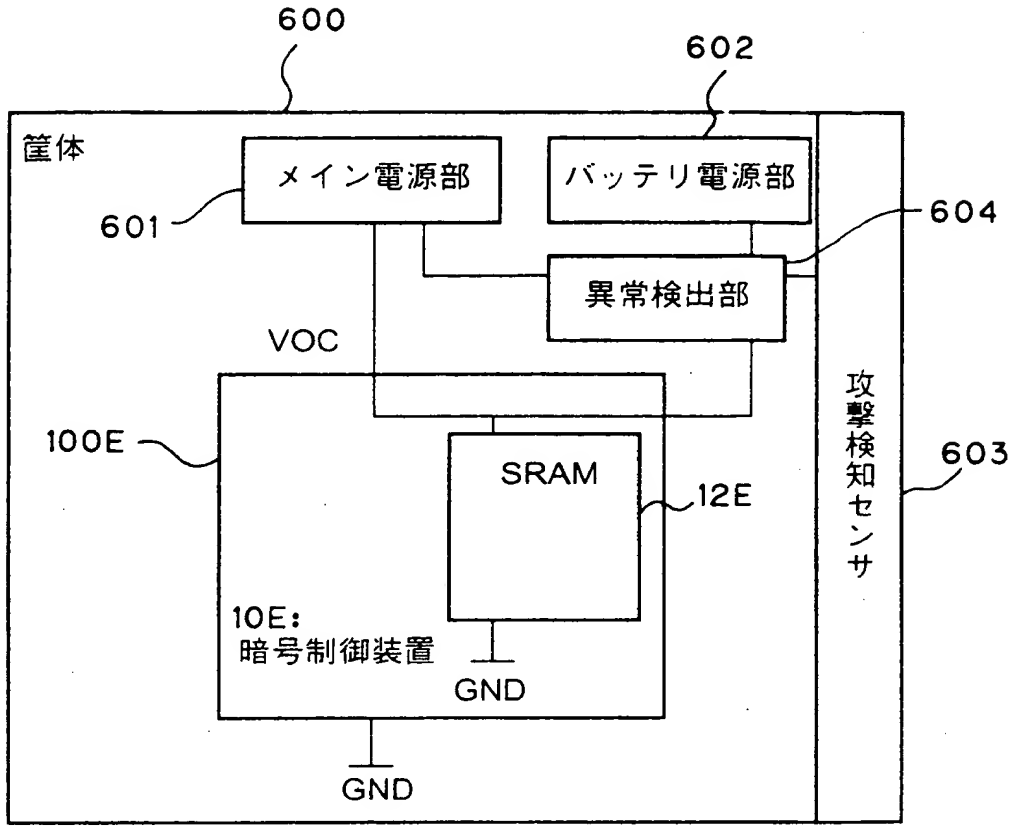

認証データ
ID
パスワード
コマンド
I/O情報

【図１１】



セキュリティレベル	アクセス権
0	アクセス権なし
1	リードオンリー
2	レベル3より一部制限
3	フルコントロール

【図１２】


600
602
筐体
メイン電源部
バッテリ電源部
601
604
異常検出部
VOC
100E
SRAM
12E
攻撃検知センサ
603
10E:
暗号制御装置
GND
GND

【書類名】　　要約書

【要約】

【課題】本発明は、データの暗号化や復号化を担う暗号制御装置に関し、データの不正な解読や漏洩を防止し、データの安全性を向上させる。

【解決手段】プログラムを実行するＣＰＵ１１Ａと、ＣＰＵで実行されるプログラムが格納されたＲＯＭ１３Ａと、ＣＰＵでのプログラム実行中の作業領域として使用されるＲＡＭ１２Ａと、外部機器との間のデータの送受信を担うＩ／Ｏ部１４Ａと、暗号化されたデータの復号化および平文のデータの暗号化を担う暗号部１５Ａとが１つの半導体素子上に形成されている。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社